



Panda Adaptive Defense 360 technologies

Managed Detection, Managed Mitigation





© Adaptive Defense 360

Index

1. Technologies and Services. Introduction
2. EPP Technology Stack
3. The 100% Attestation Service
4. Protection against application exploits and Living-off-the-Land attacks (LotL)
5. The Threat Hunting Service
6. Certifications, awards and contributions




1. Technologies and services in Panda Adaptive Defense 360.

Introduction

This document explains how the **technologies and managed services integrated in Panda Adaptive Defense 360** work together. The Endpoint Detection and Response (EDR) capabilities, and the leverage of AI technologies are differentiating factors.

The following graphic shows where each technology works and the techniques used to block adversaries as quickly as possible, preventing endpoints from being compromised, and detecting, containing and responding to attackers before damage is done.



Unattended & Managed services	PREVENT	DETECT	HUNT	INVESTIGATE/ FORENSIC	CONTAIN/ REMEDiate	ANTICIPATE Avoid Future Attacks
KNOWN & UNKNOWN MALWARE	Traditional EPP technologies ¹ 100% Attestation Services ² Risk-based Application Control: Lock/Hardening mode			Incident Analysis, Event timeline	Execution denied, Managed disinfection	Incident analysis insights  Panda Patch Management  Advanced Reporting tool  Panda Data Control
EXPLOITS Metaexploits, Exploits kits, Exploits in the wild	Pre-execution IoAs of exploits in the wild ³	Behavioral IoAs in memory ⁴	Threat Hunting & Investigation Service (THIS) ⁷		Compromised process killed, Isolate endpoints	
LIVING-OFF-THE-LAND High confidence malicious activity	Context based pre-execution IoAs (Interpreters, scripts, macros) ⁵	Behavioral IoAs with admin tools, scripts, shellcode injections ⁶			Feeds new IoAs to the endpoint agents	

The prevention, detection and response technologies and services, integrated in Panda Adaptive Defense 360, are as follows:

- 1. Endpoint Prevention technologies (1).**
- 2. Managed 100% Attestation Service (2),** which classifies all applications and binaries before and during execution, to ensure that only trusted executables can run.
- 3. Technologies to detect exploits and Living-off-the-Land (LotL) techniques (3, 4, 5, 6).** LotL techniques are used by attackers to leverage pre-existing and legitimate administrative applications with dual use, in devices and servers, and abusing them, inadvertently to the administrator.
- 4. Managed Threat Hunting Service (7),** as part of the solution. Security experts discover new LotL techniques and include these new detections in the endpoint agent.

2. EPP Technology stack

EPP Proactive Technologies Stack	Panda Adaptive Defense 360
Generalist signatures and Heuristics	✓
Cloud Based Lookup to the Collective Intelligence (Threat Intel)	✓
Behavioral analysis & IoAs detection	✓
Firewall, IDS/IPS, Networks packet inspection	✓
Anti-tampering	✓
Device Control	✓
URL Classification & Reputation	✓
Application Control	✓
Antispam, Antiphishing, content filtering for MS Exchange Servers	✓
Mailbox protection & Intelligence Scan for MS Exchange Servers	✓
Vulnerability Assessment & Patching*	✓

*Panda Patch Management

There is a common misconception in the market about EPP technologies, believing they are just traditional, signature-based anti-virus, and that they can be replaced by an EDR solution.

In reality, these technologies, besides signature-based analysis, combine generic signatures, heuristics, firewall, URL reputation, behavior and IoA analysis (Indicators of Attack), vulnerability management, application control, and other capabilities which can greatly mitigate risk.

These prevention technologies, which work together with EDR solutions, bring important benefits, among them:

- **Significant risk reduction.** They don't need to run a file to detect malware, and they only need connectivity to query the cloud.
- **Very low level of false positives.** EPP technologies, which can protect autonomously, are widely distributed in a large number of endpoints, and are configured to minimize false positives.
- **Performance optimization.** They work together, integrated, to avoid redundancies and minimize any performance impact in the endpoints they protect.

3. The 100% Attestation Service.

AI as disruptive innovation in security

A managed service is included as part of the license of **Panda Adaptive Defense and Adaptive Defense 360**, a service which classifies as malware or as trusted, all processes which execute in each endpoint. Only trusted ones will be able to run. Since it is a fully automated service, it does not require any input or decision from the end user, or from the Security or IT teams.

The 100% Attestation Service has three key components:

1. Continuous monitoring of endpoint activity, from a cloud-native platform.

Continuous monitoring of endpoint activity, from a cloud-native platform.

The activity of every application at the endpoints, regardless of its nature, is monitored and sent to the cloud for its continuous classification. This way, malware executions, and even sophisticated threats, such as Supply Chain Attacks, can be prevented.

2. Automated, AI-based classification.

Automated classifications are made in a cloud-based AI system, where an array of multiple ML algorithms is run, processing hundreds of static, behavioral and context attributes are processed, in real-time.

Attributes are extracted from the telemetry of the protected environment, and from a set of **physical sandboxes** in which executable files are detonated.

Today, the rate of automated classification is 99,98%, so that only 0,02% of the processes need intervention from our experts. The AI classification system is therefore self-sufficient, scalable to large volumes of files, working in real-time and without relying on any input from the end-user.

What is physical sandboxing?

An array of cloud-based custom made machines specifically configured to detonate files and extract real-time behavioral and contextual observables.

We use physical sandboxing instead of Virtual Machine Sandboxing, because there are numerous malicious applications that are VM-aware, detecting when they are being run inside a VM, inhibiting their malicious behavior.



3. Risk-bases application control.

It refers to the modes of operation of the Protection agent running at the endpoints. There are two levels of Protection:

- **Hardening mode:** default-deny for any unknown application or binary coming the outside (web downloads, email, removable media, remote locations, etc.).
- **Lock mode:** default-deny for any unknown application or binary, regardless of its origin (from the network, from within the endpoint itself, or from the outside). It ensures that all running processes are trusted.

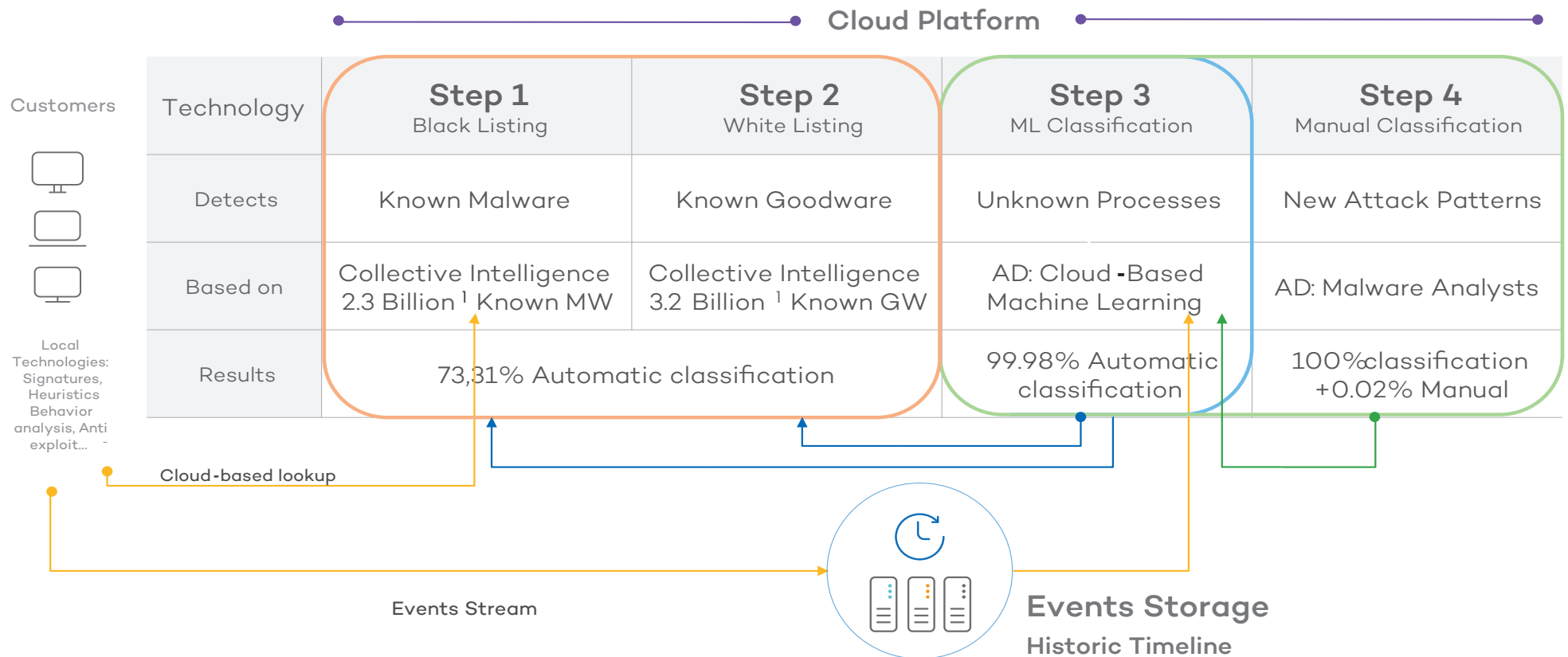
Panda Security's Collective Intelligence. Hosted in a cloud-based platform, is another key component which enables the operation of the new protection model, and which increases the efficiency of the 100% Attestation Service.

The Collective Intelligence represents the consolidated and incremental knowledge repository of all applications, binaries and other files containing interpreted code, both trusted and malicious.

This repository in the cloud is continuously fed by the AI system and by the expert analysts, and it is at the same time continuously being queried by the solutions and services of Panda Security, prior to any execution.

- The following graphic shows how the technologies in the stack seamlessly work together, enabling the classification of all applications, binaries and files with interpreted code, in real-time.

How the 100% Attestation Service works



4. Protection against application exploits and Living-off-the-Land attacks (LotL)

The continuous monitoring of the activity at the endpoints allows the agent to act as a sensor and inform the cloud platform not only about the files being run, but also about their context of execution (what happened right before, which users are trying to run which command or application, which network traffic is generated, which data files are being accessed, parameters, etc).

This allows the identification, first at the endpoint, of abnormal behaviors or suspicious and their categorization as Indicators of Attack (IoAs), with a high degree of confidence and without false positives.

Many times, IoAs are related to specific phases of the **Cyber Kill Chain** or to the tactics of the **MITRE ATT&CK framework**¹:

- Initial Access
- Execution
- Persistence
- Privilege escalation
- Defense evasion
- Credential Access
- Discovery
- Lateral movement
- Collection
- Command and Control
- Exfiltration
- Impact

The detection of IoAs, before data is exfiltrated (or encrypted in the case of a ransomware attack), is a very effective defense mechanism, and especially against Living-off-the-Land (LotL) attacks, even if endpoints may have already been compromised.

Panda Adaptive Defense and Panda Adaptive Defense 360 integrate, within the same Protection agent, a complete technology stack to detect IoAs in different attack phases. Far from being static technologies, they are updated continuously with new attack patterns and techniques, which are discovered by the Threat Hunting and Investigation Service (THIS).

Adversaries are increasingly adopting living-off-the-land techniques, present in most targeted attacks. There are four main categories of these techniques:

- Attacks using dual use software, such as PsExec.
- Memory-based attacks, such as Code Red.
- Attacks using persistence techniques, such as using Visual Basic Script in the Registry.
- Attacks using non-binary files, such as Office documents with macros or scripts.

Among the numerous Indicators of Attack that the agent detects, we find the following categories:

1. IoAs of exploits in the wild

Through these behavioral and context IoAs, exploits in the wild, as well as exploit kits are detected and blocked prior to execution, closing one of the main entry vectors for attackers.

Additionally, using proprietary “**Virtual Patching**” firewall technology, attempts to exploit vulnerabilities are detected and blocked, by monitoring inbound traffic.

As an example, this technology is used to identify and block exploits against the EternalBlue vulnerability (BlueKeep attacks), in which specific connections are established within an RDP session. These connections, unless they are blocked, allow an attacker to remotely execute code (RCE).

The Virtual Patching technology detects such connections and rejects them automatically. Detections are recorded in the cloud and presented in the web interface of Panda Adaptive Defense 360, allowing administrators to immediately take action.

They can, as a containment measure, apply configuration changes, for example, activating Network Level Authentication (NLA), or

disabling non-essential RDP services at the endpoints, or patching the systems if possible, and effectively reducing the attack surface.

2. In-memory IoAs: dynamic anti-exploit technology

Panda Adaptive Defense 360 incorporates dynamic anti-exploit technology.

This technology, integrated in Panda Adaptive Defense 360, is independent of the technologies in Microsoft’s EMET, and it is not based on any morphological analysis of the files, or on additional protections against exploit techniques not covered by Windows (ASR, EP, EAF, etc.), or on specific detections against known vulnerabilities. These techniques are not sufficient to stop attacks designed against zero-day vulnerabilities.





The dynamic anti-exploit technology monitors the internal behavior of processes, searching for anomalies. This is highly effective, regardless of the exploit used in the attack, and it is complemented with a proprietary **memory framework analysis**, which inspects a section of memory at certain times, after some specific events or behaviors are triggered. This way, new attack patterns of different types can be discovered.

These technologies can effectively protect against **any type of exploit**, particularly zero-day exploits targeting:

- **Vulnerabilities in web browsers:** Internet Explorer, Firefox, Chrome, Opera and others.
- **Common applications** often used in targeted attacks, such as Java, Adobe Reader, Adobe Flash, Microsoft Office, multimedia players, etc.
- **Vulnerabilities in unsupported operating systems**, such as Windows XP and others.

3. IoAs to detect Living-off-the-land attacks and malicious use of administrative tools.

To detect this type of indicators, events of scripts executed by script interpreters are correlated (Powershell, Visual Basic, Javascripts, etc), as well as macros/scripts in MS Office, WMI activity, etc.

Other indicators are included, to deny execution of certain processes by other processes, depending on the context, blocking malwareless attacks using administrative tools and command-line sequences. Also, some other in-memory attacks are detected, such as detections of code injections in memory without files on disk.

5. The Threat Hunting Service: Revealing the undetectable.

The Threat Hunting and Investigation Service, included in Panda Adaptive Defense and Panda Adaptive Defense 360, is operated and managed entirely by Panda Security's analysts.

They operate a cloud-native, proprietary platform for Threat Hunting and Incident Response, to coordinate L1, L2, and L3 analysts, as well as hunters and incident responders, to minimize MTTD and MTTR (Mean Time To Detect and Mean Time To Respond).

Analysts may also create new rules representing new IoAs. These high-confidence IoAs can be delivered to the endpoints, protecting, as early as possible, against adversaries bypassing other controls with techniques such as fileless, LotL, etc.

These new indicators of attack are the result of a continuous process to discover Threat actors, using advanced data analytics, our proprietary Threat intelligence, and the expertise of our analysts.

This service inherits all the cyberintelligence that we have perfected thanks to our years of experience in threat research, the historical visibility offered by the registry of the behavior of applications, users and machines for more than 30 years, and our alliances with international organizations such as the Cyber Threat Alliance, where we exchange Indicators of Threats (IoAs and IoCs) and their corresponding responses.



6. Certifications, awards and contributions

Panda Security regularly participates in and receives awards for protection and performance from Virus Bulletin, AV-Comparatives, AV-Test, NSS Labs Panda Adaptive Defense achieved the EAL2+ certification in its evaluation for the Common Criteria standard.

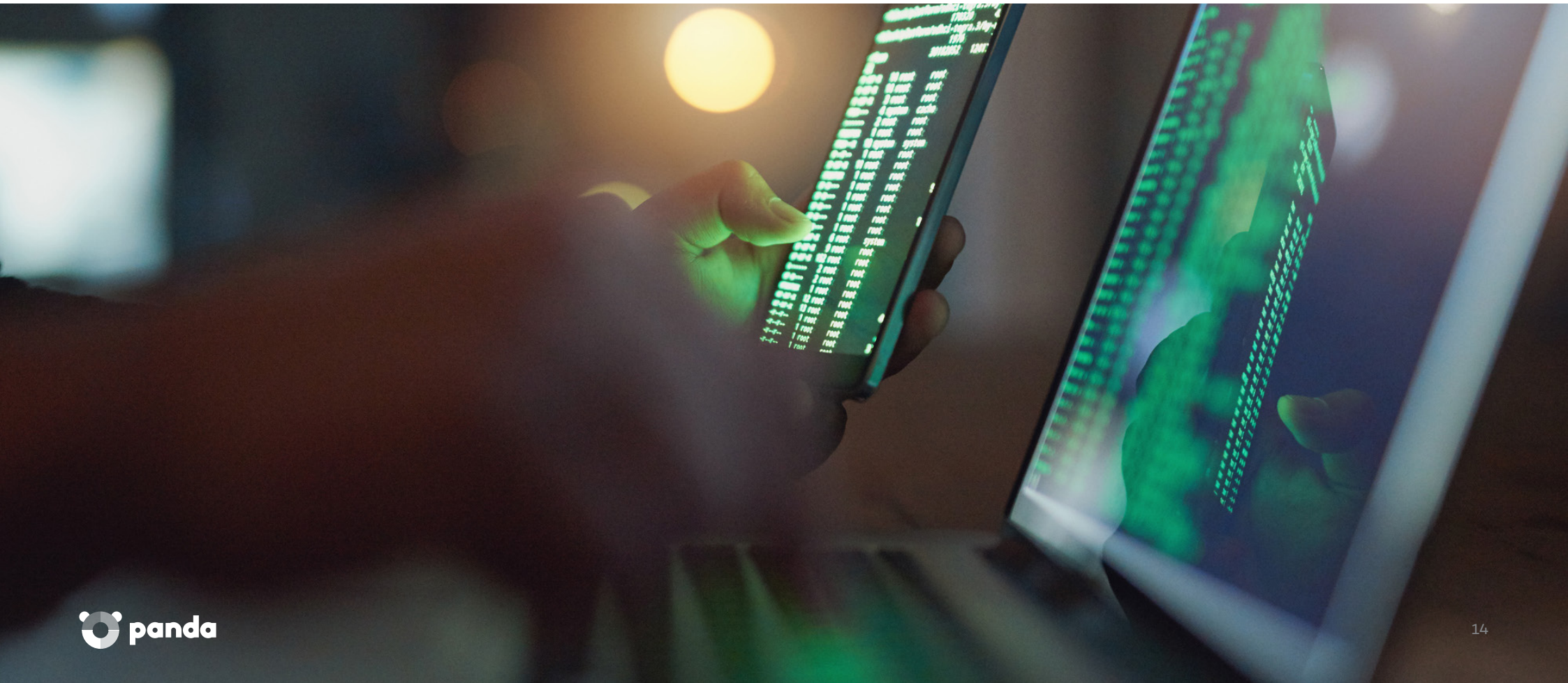


Panda Security acknowledged as 'Visionary' in the Gartner Magic Quadrant for Endpoint Protection Platforms (EPP) 2018.

**CONTRIBUTING
MEMBER**

Notes:

1. Attacks on the supply chain are an emerging threat that targets developers and software vendors. The goal is to access source codes, create processes or update mechanisms by infecting legitimate applications to distribute malware
2. MITRE ATT&CK Framework: <https://attack.mitre.org/>



More Information:

pandasecurity.com/enterprise/solutions/adaptive-defense-360/



Panda Adaptive Defense 360

Limitless Visibility, Absolute Control